Abstract
Do the deviant acts carried out by the collective known as Anonymous qualify as vigilante activity, and if so, can they be justified? Addressing this question helps expose the difficulties of morally evaluating technologically enabled deviance. Anonymous is a complex, fluid actor but not as mysterious as popularly portrayed. Under a definition of vigilantism that includes reprobative punishment rather than violence as a key element, Anonymous are vigilantes. Many of its Ops can be justified in view of the mismatch between formal norm enforcement practice and Internet natives’ experience of it. Anons are more like eco-warriors than terrorists. While their actions are contentious, their force is framed in a vision of common good that is not unreasonable. Engaging with online deviants is shown to be a productive way of identifying the weaknesses in concepts underpinning moral evaluation of Internet-enabled phenomena.

Keywords: hackers; vigilantes; punishment; DDoS; violence online; deviance; cyber attack; ethics online; internet activism; digital revolution

Do the deviant acts carried out by the collective known as Anonymous qualify as vigilante activity, and if so, can they be justified? The complexity of addressing this apparently straightforward question helps expose the difficulties of morally evaluating technologically enabled deviance, particularly when made possible by the Internet. I do not intend to provide a full moral evaluation of Anonymous. As shall become clear, that would require substantial refinements to several concepts relevant to moral evaluation. My aim is to provide an exemplar of how engagement with, rather than disavowal of, digital deviants can serve the purpose of such refinements. The revision of the notion of vigilantism, and its possible justification, is but one

*Correspondence to: Philip Serracino-Inglott, TU Delft (TBM), P.O. Box 5015, 2600 GA, Delft, The Netherlands. Tel: +31 (0)15 27 89 962. Email: P.SerracinoInglott@tudelft.nl
The title refers to an essay by Pynchon in which he is ostensibly trying to rehabilitate the name of the Luddites, but is also discreetly warning of the dangers of unbridled techno-scientific enthusiasm; Thomas Pynchon, 'Is It O.K. To Be a Luddite?', The New York Times Book Review, October 28, 1984, http://www.nytimes.com/books/97/05/18/reviews/pynchon-luddite.html.

©2013 P. Serracino-Inglott. This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License (http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
instance of the implications Internet technology has upon concepts grounding ethical evaluation.

To explain what Anonymous is, I draw attention to the research of Gabriella Coleman.\(^1\) She shows that Anonymous is not as obscure as popular discourse would lead us to imagine. Coleman’s work makes it clear that it is incorrect to dismiss Anonymous as mere criminals or terrorists. However, the phenomenon is unquestionably complex, multi-faceted, and fluid.

In the second and third sections, I focus on vigilantism, and ask if the label is applicable to Anonymous. A major problem with classifying Anonymous as vigilantes is that the definition of vigilantism I start with requires the use of violence. Due to the intangible nature of cyberspace, unless we adopt a very wide concept of violence, Anonymous cannot be a vigilante organisation under such a definition. But is violence really a necessary component of vigilantism? Considering the expressive and punitive aspects of non-violent vigilante like activities by Anonymous the definition is improved by moving away from its requirement of physical harm, and shifting focus to the punitive elements of vigilantism. Under a concept of vigilantism tied to punishment rather than violence, many of Anonymous’ actions are clearly vigilante.

This opens up the question whether Anonymous’ vigilante action can be morally justified. The answer depends on how well matched the normative impetus, or ethos, of Anonymous is to the normative positions held by those who share the same action space. A definitive answer can only be given for specific cases. Nonetheless, in the fourth section, I draw some general observations that tend to apply to an increasing number of cases as Anonymous evolves. When there is a severe ‘scale mismatch’ between what formal institutions can deliver and the requirements of justice, vigilante action can be justified.

By way of conclusion, I compare Anonymous to the Luddites, to reiterate the urgency of updating the concepts underlying moral evaluation in the face of the Information Revolution. This task can only benefit from engaging with deviants online.

**WHO IS THIS ANONYMOUS ANYWAY?**

‘Anonymous’ makes one point very clear: they do not want to be identified. However, Coleman’s persistent anthropological research provides good insight into who this collective is, how it behaves, what motivates the individuals who associate with the label, and the many complexities of Anonymous. She traces its history since birth as just a moniker for pranksters on the infamous 4chan online bulletin board. It is noteworthy how a phenomenon that today is capable of grabbing headlines was born in a virtual space known for its chaotic and infantile behaviour. The paradoxical nature of 4chan is a good place to start understanding what gives Anonymous its peculiar character. ‘4chan presents a mode of being online enveloped in anonymity and shaped by contingency. It stresses otherness, dissent, creativity, variation and plurality.’\(^2\) Unfortunately, there is not the space here to give a proper account
of how Anonymous has evolved from that early form into what it is today. What follows is merely a selection, from a much richer account, of points salient to the rest of this analysis.

Anonymous have been responsible for spiteful and mischievous personal acts, but also for thought provoking activities of critique, such as coordinated attacks on the church of Scientology. Their recent activities have clearly been much more political, as exemplified by the attacks against oppressive regimes during the Arab spring. By surveying the whole spectrum, Coleman provides a very rich picture of the collective.

Anonymous includes hard-core hackers as well as people who contribute by editing videos, penning manifestos, or publicizing actions. Then there are myriad sympathizers who may not spend hours in chat rooms but will heed commands to join DDoS attacks and repost messages sent by Anonymous Twitter accounts, acting as both mercenary army and street team. Anonymous has developed a loose structure, with technical resources such as Internet Relay Chat (IRC) being run and controlled by a handful of elites, but these elites have erected no formal barriers to participation like initiation guidelines or screening processes, and ethical norms tend to be established consensually and enforced by all.3

The processes of management and coordination of Anonymous are not formalised, much less codified. These vary depending on the circumstances. The ideas and practice of the Internet Engineering Task Force’s approach known as ‘Rough consensus and running code’ and the methods used by the ‘Occupy’ movement are the closest formalised and documented methods to the practice that Coleman is describing.4 Due to the loose structure of Anonymous, diverse methods can operate at different times or by different sub-groups at the same time.

A common metaphor used to describe Anonymous is that of the Hydra, the dangerous mythical creature with many heads that cannot be killed. Just like the hydra’s many heads, each Anon5 or sub-group of Anonymous operates with relative autonomy and destroying any single one is useless.6 ‘To be sure, Anonymous is not a singularity, but is comprised of multiple, loosely organised nodes with various regional networks in existence. No one group or individual can control the name and iconography’.7 This disjointed but collaborative nature of Anonymous is one of its main characteristics.

Operations don’t simply spring out of the ether and can be easily linked to a particular network, such as AnonOps, AnonNet, or Voxanon to take three of the most important ones today. At minimum, these networks usually will lay claim to, or deny, the source of an operation. Anons are also not completely or always as veiled, as they are often portrayed: there are regular participants, cloaked under pseudonymity rather than anonymity, and often available on stable Internet Relay Chat servers where one can interact with them every day.8

Anonymity and pseudonymity are part of the culture of this movement, not merely a means of protection against recrimination. This culture is built upon the importance attached to the ability to express oneself freely. The group is opposed to individual celebrity9 and highly values communal processes of generating knowledge. Personal privacy is paramount. Being ‘doxed’, that is, having one’s personal details published
online, is perhaps the worst form of humiliation that can befall an Anon, and the community uses ‘doxing’ as a form of internal discipline/punishment. Inversely, Anonymous expects a high level of transparency from governments and corporate entities. In fact, its most spectacular exploits have involved the disclosure of sensitive information that from the perspective of the Anon ought to have been free.¹⁰

While revealing the general character traits of the collective, Coleman also repeatedly reminds us of the importance of individualism within the grouping. Whenever Anonymous speaks publicly, it directly or implicitly stresses the point that Anonymous is leaderless and that there is no sharply delineated ideological position all those who participate in its actions could unequivocally endorse. It seems that the very diversity of interpretation of fundamental yet supple precepts, coupled with an openness to develop a common path of action, is what brings these individuals together.¹¹

Her work hints at a normative sub-structure. This picture of Anonymous is very different from that which is typically presented by the media or political and commercial actors. ‘The impossibility of forming any comprehensive, consistent picture of Anonymous is precisely what makes the group so unsettling to governments’.¹² Anonymous has been portrayed as a chaotic bunch of misdirected immoral but technically skilled deviants. ‘Cyber-vigilantes’, ‘terrorists’, ‘hackers’, ‘anarchists’ are all terms that have been used, almost interchangeably, to try to box this phenomenon into a familiar notion.¹³

By painting Anonymous as so inchoate we not only empirically misrepresent them; we drift inevitably into hyperbole, exaggerating the extent to which people find them threatening, adding to the air of mystery surrounding hackers who fly under that banner, feeding into the hysteria that law enforcement (and the defence contractors selling security and ‘anti-hacker solutions’) self-consciously seek to cultivate.¹⁴

Because of the fluid nature of Anonymous, any general claim about the group can probably be counteracted with at least one example that does not fit the model. However, each of Anonymous’ Ops¹⁵ is rather specific in its motivations. I will focus on more recent major Ops. As Anonymous is still an evolving phenomenon, it is reasonable to focus attention on the leading edge of this evolution. This is not to say that their heritage is to be ignored. Their path of development is also highly informative. But their more recent activities involve larger numbers of individuals, so it is reasonable to assume that they reflect prevalent online culture better.

ARE ANONYMOUS VIGILANTES?

This analysis looks at a single aspect of a multi-faceted phenomenon. Nevertheless, it is sufficient to sustain a general claim that revision and improvement of moral frameworks in the face of the issues raised by Internet technology can benefit from the analysis of deviance online.
Coleman lists ‘cyber-vigilantes’ as one of the imprecise derogatory terms applied to Anonymous. Vigilantism is not necessarily immoral or unjustified. The term vigilante is used in common discourse to describe some fictional heroes (e.g. Batman or Dirty Harry) who defend the weak when the law fails them. Anonymous’ exploits such as ‘Operation Payback’ against credit card companies in response to the way these dealt with Wikileaks seem to fit roughly this model, especially to those who find that Wikileaks was treated unjustly in this case. In another instance, when Anonymous revealed the details of a man they claim cyber-bullied a teenager to suicide in Canada, the Canadian Mounted Police warned of the dangers of ‘vigilantism’. While the term was used pejoratively in this case, the actions fit the general conception we have of fictional vigilante heroes. To find out to what extent the intuition that Anonymous are vigilantes is correct, I shall rely on Travis Dumsday’s refinement of the definition provided by criminologist Les Johnston. According to Dumsday:

Vigilantism is the organised use of violence or threat of violence by an agent or agents who are not willingly accountable to the state, for the purpose of controlling (preventing and/or punishing) criminal or noncriminal but still deviant actions; which violence or threat of violence is directed specifically against the perpetrators or alleged perpetrators of those actions, in accordance with the vigilante’s own system of minimally defensible values, the motivation for which must include what the vigilante perceives to be a concern for justice or the good of the community.

This definition yields five criteria that must be met for an action to count as vigilante, namely, it must:

1. be conducted by agents not willingly accountable to the state
2. be an organised or premeditated action
3. be in accordance with the vigilante’s own system of minimally defensible values
4. be motivated by a concern for justice or the good of the community
5. use violence directed specifically at the infringer of norms.

Anonymous’ actions do not fully satisfy these criteria. They fail to satisfy the criterion of violence, simply because the space within which they operate is an informational not a physical space. Other than that, when the actions of the collective are dissected, it is evident that Anonymous does, in all respects but violence, fulfil the criteria of the definition. In the next section, I will explore the changes needed to the definition if we are to retain the classification of vigilante for Anonymous. The full force of the original definition is retained if the requirement of violence is replaced with a requirement of reprobative punishment. This broadens the scope of the definition enough to account for activities in cyberspace without losing selectivity. But before that, in the rest of this section I will examine the first four criteria in turn to see how they are satisfied by Anonymous’ actions.
Agents not willingly accountable to the state

Anonymous is not willingly accountable to any state. In fact, Anons are generally antagonistic to states. Anonymous has launched a number of very localised actions in connection with rape cases in which the suspected perpetrators went unpunished.\textsuperscript{21} The media reported these cases as Anonymous ‘taking on’ a township.\textsuperscript{22} While in one case citizens who dared counter the Anonymous position where also attacked as rape apologists,\textsuperscript{23} the true focus, and the brunt of the attack was directed at the apparatus of state. One of videos on YouTube relating to the Maryville case could not be more explicit: ‘If Maryville won’t defend these young girls, if the police are to cowardly or corrupt to do their jobs, if justice system has abandoned them, then someone else will have to stand for them. Mayor Jim Fall, your hands are dirty. Maryville, expect us’.\textsuperscript{24} Town hall websites have been hacked, and prosecutors, sheriffs and other law enforcement or justice system officers harassed. This class of Ops makes it amply clear that the ‘failing justice system’ is the enemy. Even if what Anonymous ultimately seeks is for that same system do what it is supposed to, hold perpetrators to account for their misdeed, no Anon is willingly accountable to that authority for their online activity against it.

Other Ops, the kind that propelled Anonymous into the headlines the world over, are much wider in scope. Problems with evaluating this requirement will arise whenever potentially vigilante action takes place somewhere with unsettled sovereignty claims. Anonymous’ activity in connection to the Arab Spring occurred in a sphere where there was a breakdown of the system one would have to be accountable to under this part of the definition. The very same person might be promoting an anti-government protest in an oppressive regime in the morning, and participating in a Distributed Denial-of-Service attack (DDoS) on a city hall website in the afternoon, from a computer half a world away from both, through a proxy server in yet another jurisdiction. To which state is such an individual to be accountable for being an Anon? Large-scale events in cyberspace are state-transcending in the same way that notions such as the Common Heritage of Mankind, agreements like the Law of Space, or problems like climate change are. In such cases, the pre-supposition of an immutable state is more of a hindrance than a useful notion. Moreover, in the case of cyberspace the scale and speed of effects, particularly in terms of public engagement, is so massively larger than any previous phenomenon that concepts such as ‘the role of the state’ emerge more readily as points of contention.

As Anonymous becomes more clearly political it is condemning the existing apparatus of state as defective much more explicitly.\textsuperscript{25} But demands for effective state-served justice, as in the rape cases, show that not all Anons are opposed to the idea of the state \textit{per se}. So one must not fall into the temptation of declaring the state passé, an irrelevant concept to be overcome in the information age. That would be unrealistic given that for the foreseeable future the nation-state and cyberspace will coexist. However, when dealing with issues raised by advances in Information and Communications Technology (ICT), we must constantly re-open and critically evaluate the notion of the state. Inquiry in this vein is to be found in the ecological movement,
and also in attempts at formulating governance structures for spaces beyond the territories of states (Outer Space, Radio Waves, the Ocean Floor, etc.). While studies on the effects of the Internet on the sovereignty of states are available, analyses of how the very concept of ‘state’ affects netizens’ lives online are hard to come by.

Organised or premeditated action

The requirement of organisation or premeditation serves to exclude cases of self-defence or spontaneous altruistic interventions. Johnston makes it clear that only a minimal level of organisation and premeditation is required. He concedes that there can even be lone vigilantes. While the amount of pre-planning required can be minimal, it is a necessary component of any vigilante action; otherwise, the notion would become conflated with all kinds of vengeance and with reactive self-defense. Anonymous uses online communication to coordinate geographically distributed individual’s attacks on pre-selected targets. Therefore, even from casual observation, it is clear that Anonymous’ actions meet this requirement of the definition.

While this criterion is easily satisfied, Anonymous’ organisation is not conventional. As with other online phenomena such as the Open Source Software movement or Wikipedia, an increasing number of online phenomena continue to challenge our understanding of how people organise themselves to undertake collective action. Unless we can go beyond simple hierarchical schemas and assumptions of rational-egoist actors to explain human cooperative action, making sense of diffuse entities such as Anonymous will be very difficult, if not impossible. While scholars have been researching complex arrangements used for common action for several years, the hierarchy of command is still a dominant notion. The need to deal with ICT-mediated events such as those featuring Anonymous highlights the importance of new conceptual tools for analysing unconventional organisational arrangements.

The vigilante’s own system of minimally defensible values

Vigilantism must be in reaction to a violation of norms or pre-emptive of a potential violation. More precisely:

what is required ... is simply a concern on the part of the vigilante for what he or she sees as justice or the good of society, whether those values pertain to the attempted enforcement of positive law, natural law, societal custom, or all three. ... In fact, a vigilante can defend a system of values unique to himself. ... However, there are some limits on this. I believe that in order to keep the vigilante label, the value being defended must be one that an ideally rational agent would regard as at least arguably worth defending.

Some of the targets chosen by Anonymous have been criticised as behaving in ways that are detrimental to society. Some online commentators argue that Wikileaks is beneficial to society and democracy. They might not condone Anonymous’ behaviour, but would consider actions taken by governments and private companies against Wikileaks as exactly the kind of norm violation referred to by Dumsday.
It is in reaction to these actions that Anonymous launched one of its biggest attacks. Similarly, the practice of threatening with lawsuits downloaders of copyrighted material might strictly be within the bounds of law, yet, many think of it as a form of extortion. The popularity of the Pirate Party indicates that viewing such copyright enforcement tactics as anti-social behaviour is a defensible position. So the system of values Anonymous is fighting for is minimally defensible.

Arguing that Anonymous’ values are minimally defensible by inference from the presumed norm infringement of their targets does not reveal what these values might be. An ethical framework which could cover the system of values that are important to the wider community of which Anonymous is but the strong-arm still needs to be developed. Since individual Anons prioritise different sets of values, it is difficult for any single ethical theory to provide complete coverage. What can be described is some basic conceptual structure upon which differing ethical positions can be sustained—one that can be reasonably ‘retrofitted’ as coherent with the actions without claiming that it would have been a motivation for such acts. While all members of Anonymous will never be of a single opinion on the morality of a specific act, they must at least share the rudimentary normative structure which allows them to recognise each other mutually as Anons (or by which to confront others for not being Anons).

In blogs and forum posts by or about Anonymous, there are often references to a ‘hacker ethic’ or ‘hacker culture’. The hacker ethic is not a well-defined system of ethics, but a term that tries to capture the Zeitgeist of a class of technically inclined netizens. Once again, we need to extrapolate normative positions from the entities Anonymous tries to protect. Since Anonymous actively supports Wikileaks, one can presume that their ideologies overlap. Anonymous’ ideology must include some form of the radical transparency for institutions paired with strong privacy for individuals that is at the core of Wikileaks’ ideology. The radical transparency advocated by Wikileaks is conceptually not far from the mantra of the hacker ethic: ‘Information wants to be Free’. Similarly, the importance of pseudonymity is related to ideals of non-discriminatory meritocracy, a fundamental principle for the Open Source movement. But such notions remain vague. Attempts to explain the Open Source approach in an instrumentalist fashion are informative, but do not extend well to non-programming activities.

Wikileaks does claim a consequential benefit for its actions (undermining totalitarian regimes and corrupt governments, etc.), but its method would be oddly arbitrary if it were not tied to the value of public information. The whole Wikileaks project could be premised upon the primacy of certain kinds of information objects (the leak, or the cable), which must be set free; such information has a proper place (in public view) and keeping it hidden and locked away is intrinsically immoral. The motivations of Anonymous also seem to be based more on principle than utility. Yet the context sensitivity and rapid position changes typical of Anonymous, place it at some distance from any formal deontological position. An information-centric conceptualisation of morality would be most useful.

Such a theory is Luciano Floridi’s Information Ethics (IE). This approach seems very well suited to expressing the common sentiment of Wikileaks and Anonymous’
core ideologies. ‘Information wants to be Free’ can be reinterpreted in IE terms as the ‘flourishing of information objects’. Thus ‘leaks’ are relocations of information objects of high value to an environment (the public domain) where they can flourish properly.

Consider Floridi’s four universal laws against information entropy:

1. information entropy ought not to be caused in the infosphere
2. information entropy ought to be prevented in the infosphere
3. information entropy ought to be removed from the infosphere
4. the infosphere ought to be protected, extended, improved, enriched and enhanced.

Actions intended to disrupt online services cause information entropy in that slice of the infosphere known as the Internet. But before condemning Anonymous for their entropy generating activity, one has to consider if their targets are guilty of greater entropy generating actions. If Anonymous’ targets significantly harm the infosphere, law 4 above would place a moral obligation on those who have the resources (e.g. elite hackers) to protect the infosphere and to intervene even as vigilantes. The information entropy generated by the attacks is unavoidable ‘collateral damage’ of actions aimed at limiting the higher-order entropy generated by the targets’ services. Draconian copyright enforcement, censorship, the spread of pseudo-scientific mythologies, or an institutionalised lack of government or corporate transparency can all be conceived as entropy generating, and these affect the entire infosphere, not merely the online digital part of it. The ecological approach embedded in IE allows us to conceive of Anonymous as eco-warriors whose environment is the infosphere. This approach does not exonerate Anonymous from moral responsibility, as eco-warriors can also be morally problematic, but it helps conceptualise a common moral framework for a loose group of individuals with distinct value sets.

Coverage of the phenomena by an ethical theory does not mean that the actions are morally justified, only that they are defensible. That is sufficient for determining if they are vigilantes or not. Other classical theories might still allow for a more rigorous analysis, at least at the theoretical level, but they would be very problematic to apply in practice. This is because the value set of hackers is shaped by their defining activity—hacking. Online activity influences the way hackers think about moral issues. IE is the only moral theory described using the paradigms and vocabulary of Object Oriented Programming. IE provides a common language (and perhaps an evaluative structure) shared by hackers and ethicists.

Justice and community as motivation

An act is an act of vigilantism only if it is motivated at least in part by a concern for what the vigilante perceives as justice or the good of the community.

The ecological aspect of protecting the infosphere implies that Anonymous’ actions are motivated by the good of the community. Is this strong enough to qualify...
Anonymous as vigilantes? Anonymous does have a strong communitarian commitment but it is not as clearly visible as its commitment to individualism and autonomy. The communitarian spirit of Anonymous can be seen more vividly if one takes a closer look at their tools through a ‘Disclosive Ethical Archaeology’ approach.40

Let us unpack the ‘weapon’, called the ‘Low Orbit Ion Cannon’ (LOIC), used by Anonymous in most of its attacks. There are a few variants of it including a web-based version.41 This is not a particularly sophisticated bit of technology. It consists of less than 1500 lines of fairly straightforward code, a substantial part of which is for the user-friendly interface. The kind of attack it delivers is also crude. A Distributed Denial of Service attack consists in sending a massive amount of requests to a service. To achieve its effect, several attackers each send some requests then abandon the connection before receiving a reply. This is repeated over and over again, several times a second. The more attackers there are, the longer they can keep sending requests, the stronger the attack. The idea is that this will seem like a huge surge in regular traffic to a web server, but nobody is actually visiting the web pages. The requests are coming from the LOIC and then discarded. If a web server is hit with a sufficiently large number of such requests it will be overloaded. It will be unable to serve legitimate requests and thus appear offline, if not crash outright.

This is like organising a flash crowd on a bus, denying legitimate travellers the possibility of getting on. If the flash crowd is large enough the bus driver might have to stop the vehicle and delay the service. This kind of DDoS attack relies on people voluntarily joining the attack. The LOIC is inscribed with yet another communitarian element. The ‘hivemind’ feature allows quick coordination and synchronisation of several LOICs. As the LOIC README file explains ‘HIVEMIND mode will connect your client to an internet relay chat (IRC)42 server so it can be controlled remotely. Think of this as a voluntary botnet (though do beware that your client can potentially be made to do naughty things)’.43 In this case, there needs to be a high level of trust in the community, and in particular, in any leaders. Participation is not coerced such as it would be if the attack was launched from a network of compromised systems.

It has been reported that Anonymous has used botnets, and some lone members (or small subgroupings) have carried out significant attacks independently using such networks of compromised systems. Yet, community approval and support of any action is crucial to the group. Any attacks launched by individuals, or by elite subgroups, only gain their force as Anonymous’ handiwork when the community rallies behind them (I will discuss this further in the next section).

The channels of communication used by Anonymous also reveal that rational-egoist accounts cannot fully explain their motivations. The heavy use of social media already points to the value Anons place on public coordination of shared action. Their use of IRC is even more telling. Anons might justify the use of IRC as the best tool for the job, but as a technology it is severely outdated. The XMPP protocol, an open standard for chatting software with freely available implementations, would be a better choice on merits of features alone. The most popular deployments of XMPP are Facebook’s and Google’s chat systems. On the other hand, most IRC
servers are still run by volunteers. There are several such IRC networks, with none clearly dominating. *Ad hoc* IRC servers can be launched easily. The Anons’ preference for IRC indicates that they attach significant value to diffusing control of strategic assets throughout the community. Not only does Anonymous refuse to explicitly declare leaders, but their *de facto* leadership, the elite, chooses technologies that force them to rely more heavily on the wider community’s mutual support.

The choice of tools such as Pastebin (websites that allow you to paste any piece of text and get a weblink to that text) to go along with IRC also reveals that there is a harping back to a semi-mythological ‘early days of the Internet’. This would be the time when the characters from Steven Levy’s book flourished in total information freedom. Pastebin was created to make it easy for people discussing programming issues to ‘paste’ bits of code for one another to examine, without polluting the chat window with source code. It has hardly any purpose outside programmer communities. Yet Anonymous uses this technology to publish its public announcements, attack plans, and press releases. This gives the activity a retro hacker styling, a reminder of the lineage to what could be called the ‘founding fathers of the Internet’. The use of what is, in Internet terms, archaic technology, programming tools re-purposed for public relations and coordinating activity, spelling that is more arcane than SMS language, all serve to create an aesthetic that members of the community can adopt and identify with. This aesthetic also creates a porous cultural boundary. The community is fundamentally open to all, but in practice, only those with an adequate technophilic attitude can communicate effectively with peers. This barrier is porous, as this is not a secret language a sect might use. All its elements are widely and publicly documented on the web. As long as one is willing to put in some effort to become familiar with the practices and conventions, he/she is welcome.

Another example of latent communitarian commitment comes from Bittorrent, a favourite software protocol for file-sharers around the globe. Anonymous has launched various attacks against copyright enforcement agents, and in support of online infrastructures used for file sharing. Anons are most likely file-sharers themselves. This protocol goes as far as to encode fairness of exchange in its specifications and implementations. The software is designed to preferentially provide data to peers who are already sharing. The more you share, the more peers will send the data you want your way.

This is not radically different form any sub-culture adopting its own aesthetic to reinforce community spirit. The major difference with Anonymous is that the communitarian spirit and the aesthetic are technologically mediated, and where possible, inscribed as code in software tools (which according to Lessig is tantamount to law). One could counter that I am overloading the meaning of communitarianism onto technologies, which were chosen for purely pragmatic reasons. However, the purpose of disclosive ethics is not to identify causal linkages, nor to document conscious ethical considerations, which affect technological choice. It aims to trace historical evolution, reveal conditions of possibility and suggest plausible affordances of particular technology–human assemblages. It interprets the cultural milieu of some particular technology-in-use to expose hidden meanings.
that impinge upon the legitimacy and valuation of a technologically mediated human action.\textsuperscript{49} Elite hackers do not necessarily or explicitly evaluate their technologies to choose the ones which best reflect their communitarian ideals. The causal chain might also be going in the opposite direction. Anonymous might have acquired their communitarian spirit from exposure to IRC and Bittorrent, or from the demands made upon them by the LOIC. Or maybe they choose to use these peculiar tools because Anons are genetically pre-disposed to communitarian-ism. It does not make much difference to the crucial observation being made here: despite assertions of cyberspace being the new Wild West, where the lone gunman/hacker is hero and king, along with other individualistic tough talk from Anonymous, their use of technology reveals a strong communitarian component that cannot be dismissed.

**PUNISHMENT, THROUGH VIOLENCE OR SHAME**

Thus far Anonymous’ actions meet the criteria required to be labelled as vigilante. While the first two criteria are relatively straightforward, the second two require the application of innovative conceptual tools to bring into sharper focus the match between criterion and action. The last requirement, that of violence,\textsuperscript{50} is substantially more complex. Unfortunately it is the feature of vigilantism about which Johnston goes into least detail, and Dumsday adopts this part of the definition unmodified. Presumably this is because it is the most obvious component of vigilantism as commonly understood.

Since the activities under scrutiny occur online, essentially in the form of digital expressions, they cannot cause any physical harm (at least not directly\textsuperscript{51}). Under a concept of violence that requires direct physical harm to the bodily integrity of a person, there can be no online violence. One would have to conclude that Anonymous’ actions are not vigilante actions as defined by Dumsday. Yet, if violence is such an essential component of vigilantism that Anonymous’ (necessarily) non-violent nature requires rejecting the label of vigilante, why does the label persist in the media and popular discourse?

Their actions meet all other criteria for vigilante action. Above, I have argued that, whether any given Op is construed as coercion or just a nudge, Anonymous is a force for order—order according to its own normative framework, to be sure—but still a force to be reckoned with. They might not be physically violent, but their actions do carry a sufficient force, and their threats are serious enough, to invite preventive action. Perhaps we need to expand the notion of violence to include such actions. A restrictive concept of violence is certainly useful in legal contexts. Clearly violent attacks upon persons should be sanctioned more heavily than similar but-for-violence infringements. On the other hand, ‘[v]iolence is one of the most elusive and most difficult concepts in social science’.\textsuperscript{52} When one takes into account the idea held by some feminist authors that pornography is a form of violence against women, the widespread use of the notion of structural violence, or the desire to condemn
psychological bullying on par with physically violent bullying, arguably, the notion of violence is under-served by restricting it to merely physical harm.

In introducing a special issue of Global Crime on the topic of violence, Bufacchi summarises the findings as follows:

On the basis of the eight papers in this volume, we can perhaps start to draw some tentative conclusions regarding the best way to conceptualise violence. First of all, we might want to say that if there is a core to the concept of violence, this is to be found in the idea of violence as disintegration, where the term ‘disintegration’ means simply the breaking down of integrity or unity. Thus, violence can succinctly be defined as the violation of integrity (Baker; Perry; Salmi). There are many different ways of violating someone’s integrity, directly (Gross; Krause; Perry), or indirectly (Gordon; Salmi; Krause; Perry). Furthermore the disintegration can occur at the physical level (Gross; Krause) or at the psychological level (Salmi; Mizen). The violation of integrity is often done intentionally (Gross), but non-intentional harm can also amount to violence (Gordon; Krause). Finally, there is a close relationship between violence and injustice, although violence and injustice remain distinct concepts that should not be collapsed into one (Baker; Salmi; Perry), and while violence is prima facie wrong, its use may still be justified (McCormick; Baker).

Adopting such a flexible concept of violence would make it trivial to argue that Anonymous are violent actors, but it would also cast the net too wide. Without further specification, the wide notion of violence would imply that Gandhi’s movement was vigilante, as opposed to the non-violence it is known for. Such a transmutation of the concept of violence is attempted by Žižek, and it might be useful in motivating a discussion on the idea of cyber-violence. Alas, such a radical re-conceptualisation of violence is unlikely to yield a better understanding of vigilantism (and Anonymous) than what Johnston and Dumsday provide. What is being sought here is an understanding of vigilantism that applies to historic cases, accommodates common discourse about Anonymous, but still excludes enough to remain useful. Probably, the notion of violence needs to be expanded to take account of psychological bullying and other non-physical harms, as the emergence of cyber-bullying seems to demand, but that would not resolve the issue at hand. While a notion of vigilantism based on a narrow understanding of violence excludes Anonymous, one based on a wide understanding of violence would include Gandhi and the civil rights movement. Both are mismatched to intuition and common understanding of the word vigilante.

Johnston argues that vigilantism must include violence, not simply punishment, citing cases where there was violence, but no punishment imposed upon the victims. He seems to ignore the possibility of a credible threat of punishment being enough in the same way that a credible threat of violence is sufficient for cases where the vigilantes do not actually harm their target. Moreover, Johnston does not elaborate what conception of punishment he means. His analysis is based on a number cases reported in the UK media as vigilante acts which occurred in very early 90s, that is, prior to the emergence of cyberspace as a social arena. Keeping in mind that online activity is essentially expressive provides a hint of what Johnston might have missed.
The acts of (intended) violence dismissed as not punitive also carry an expressive payload. It is here that a punitive intent on the part of the vigilante can be found. When one takes into account the expressive element of punishment as discussed by Joel Feinberg\textsuperscript{56} it becomes apparent that the expression of punitive intent is no less powerful than a threat of violence for satisfying the vigilante’s concern for justice or good of their community. It is not a formalised execution that makes vigilante actions punitive, but the reprobative expression, often in the form of violence or shaming. ‘Reprobation is itself painful, whether or not it is accompanied by further ‘hard treatment’\textsuperscript{57}. While the ritualistic aspect found in most punishments makes that expression of reprobation unmistakable, all that is needed for an act to be vigilante is that the reprobation is meaningful to the community whose norms are to be protected.

\textbf{Anonymous’ force}

Is Anonymous’ force anything more than instrumental naming and shaming aimed at making the humiliated entities conform? Can online humiliation have a punitive payload equivalent to that of physical violence in the cases of classical vigilantism? A close look at various new penal trends (e.g. community notification laws, Megan’s Law and its equivalents in the United States, or Three Strikes laws) reveals a trend:

What we also see in those new forms of punishment \ldots is a repositioning of the relationship between shame and punishment. Shame in the modernist sense of this term in penalty \ldots is in retreat; in its place, shame in the postmodern sense of the term in penalty—a tactic of punishment directed again at the individual offender—gains a sturdy foothold. Shaming can thus once again come about through their public humiliation\ldots\textsuperscript{58}

Pratt concludes that to understand the contemporary framework of penalty, we need to go beyond Foucauldian terms and develop a better framework,

\ldots [one] which allows us to take more note of those sentiments and sensitivities manifested in the new trends, and those new social forces driving punishment, \ldots a greater concentration, perhaps, on the semiotics of punishment than the hidden functions thought to lie behind its bureaucratic administration—a sociology of \ldots shaming, exclusion and incapacitation—rather than the commitment to normalization.\textsuperscript{59}

Additionally, Feinberg’s understanding of legal punishment is that of a ‘\ldots conventional device for the expression of attitudes of resentment and indignation, and of judgments of disapproval and reprobation, either on part of the punishing authority himself or of those “in whose name” the punishment is inflicted. Punishment, in short, has symbolic significance \ldots’\textsuperscript{60}. Since Anonymous is not willingly accountable to the state, the punishing authority has no formally codified locus, but communitarian and diffuse as is the punisher. Anonymous’ exploits, and its use of shame,\textsuperscript{61} against corporations or individuals it judges negatively
goes beyond public pressure and ‘sending a message’. Through collective action and public exposure, a hack that is otherwise merely a technical glitch, turns into a confrontation, a ‘J’accuse!’, towards the normative position of target. It becomes, in essence, a form of reprobative punishment. The moral position is re-asserted by symbolically destroying that which most represents infringing activities. It is punitive with the same force that a state sanctioned sentencing has.

Consider one of the main kinds of action taken by Anonymous: defacement of websites. In such cases the actual damage (as measured in dollars) to the operators of the website is typically minor. Taken in isolation, website defacement and DDoS attacks, especially when such threats are subsumed into ‘the cost of doing business’, are not only not violent, they are neither forceful nor effective in enforcing any particular order.

‘Whether they have an agenda or not, they should be looked at as the same thing’, says Chris Wysopal, CTO of Veracode, a firm that provides software security testing. ‘If you’re an organisation trying to figure out if you’re at risk from one of these groups and whether you’re vulnerable, it doesn’t really matter what their motivations are. You want to make sure you’re not at risk and your corporate data’s not exposed’.62

Getting hacked is interpreted as a lack of efficiency of the digital security in place. It is a ‘white-collar crime’ so to speak, within (theoretically) measurable parameters. While this forces site owners to engineer their digital infrastructure in specific ways, it can hardly be considered any more a form of coercion than preventive measures against natural disaster are forms of coercion. It does not raise a threat of the level or kind required for vigilantism.

Although defacing of websites is typically done by lone hackers or small teams of elites, the role of the wider Anonymous community plays an important role in amplifying its effect and turning it into a public affair. This happens mainly through exposure and ridicule of the injured party. The real force of defacing a website is symbolic. When a website is defaced (or even made unavailable through DDoS) it is in a sense unmasked, the vulnerability of the technical system, and by extension the fallibility of the institution behind it, is brought to the fore. The skinless face of the entity, without the theatre make-up of marketing is subjected to the taunts and parody of the Anonymous from behind its iconic mask. The media is recruited to expose this to the wider public. This is no longer business-as-usual, it goes beyond the ‘natural’ risk of public endeavours. The kind of event that can be called ‘an attack by Anonymous’, rather than simply ‘getting hacked’, has a certain moral legitimacy in the eyes of those who share their ethical framework.

This legitimising effect through publicity is not too different from the transition from graffiti to street art. Spray painting one’s own pseudonym on a city wall, even if done creatively and in an aesthetically pleasing manner, is little more than mere vandalism. It is a technical problem that the city department responsible for cleanliness needs to resolve in the most cost effective manner possible. The solution might be harsher penalties, and stricter policing, or it might be technological, such as anti-graffiti coatings on public property. On the other hand, if the same kind of
painting technique is used to express a message relating to its context; e.g. a social message relating to that part of town; and its size, quality, or originality make it remarkable enough for the general public or the media to take note of it; or to engage other graffiti artists to reply to it in kind, that bit of sprayed paint earns a certain legitimacy, particularly with those who share the ethical framework that informs that particular work. The graffiti becomes street art. The expressive power of street art as social critique gains its power exactly from its ephemeral nature, the pseudonymity of its creators, and its deviant genesis—from being so similar but sufficiently distinct from simple vandalism. It is what we all would have wanted to try, but only a few have both the skill and the courage to do here and now. When established institutions recognise the normative framework of the street artists as legitimate, the problem of ‘cleanliness’ can be addressed through a social equity perspective, such as is the case with municipalities that earmark certain public spaces as ‘legal graffiti walls’.

There are even more forms of deviant behaviour which derive legitimacy from the expressive component of norm infringement. Certain forms of squatting and hip-hop culture feature behaviour typically dismissed as anti-social which, upon deeper inspection, is found to be forcefully expressive. These behaviours’ of expressivity contribute to shaping society positively and provide their moral justification. Deviant expressive forms, despite the damage and harm their performance might cause, can gain legitimacy as statements of disapproval of the given order, or as desiderata for a new order. This is likely to happen when deviant expressions resonate with a widely held but context-specific public moral sentiment. Just as street art critiquing unequal society might resonate with a young urbanite crowd; hip-hop songs eulogising inmates and dissing police resonate with disenfranchised inner city dwellers; and squatting is respectable in places where homelessness is rife and abandoned property plentiful; Anonymous’ exploits resonate with an ever growing segment of Internet natives who are distant from centres of political power.

Vigilantism is purposeful directed action. It seeks the good of the community it serves, and reassurance of the continuity of cherished norms. This cannot be served by violence that is not, is some way meaningful to that community, punitive. But it can be served by punishment that is not violent. In view of the above, the fifth criterion of the definition of vigilantism can be redefined as:

an action which inflicts (or credibly threatens to inflict) harm, specifically upon the infringer, with punitive intent that is reprobative under the vigilante’s own notion of justice

We can now conclude that Anonymous are vigilantes. The definition of vigilantism I start with is an example of a concept that seems reasonable and stable until we are faced with the possibilities for action offered by powerful technology such as the Internet. When viewed through the case of Anonymous the problem with making vigilantism dependent on violence emerges. The online deviance of Anonymous indicates that the fifth element of vigilantism is punishment, not violence. Just as the notion of justice to be used must be the one held by the vigilantes themselves, so too, the punishment must take a form that is reprobative in a way that is meaningful to
the vigilantes, and not necessarily on the terms of the established legal order. Is this vigilanthism justified?

**BUT IS IT OK TO BE AN ANONYMOUS?**

Vigilante action is always aimed at justice and the public good as these are conceived by the vigilantes themselves. Whether a vigilante action can be morally justified or not depends on at least two considerations: (1) is there a non-punitive (and law-based) alternative to provide peace of mind to the social group that the vigilantes aim to protect?; and (2) is the set of social norms which the vigilante action wants to protect reasonable (i.e. do they conflict with wider society’s moral framework)? These questions can only be answered with certainty on a case-by-case basis. The range of activities Anonymous is engaged with is becoming wider, and the circumstances are different for each. However, there appears to be sufficient commonalities to allow me to attempt some general observations.

**The short arm of the law**

The history of vigilantism in the Old West offers an interesting comparison to the case at hand, which helps address the question of legal or non-punitive alternatives. As the frontier moved west, the traditional forces of the law were unable to keep up. In those brutish conditions various vigilante groups emerged in the attempt to bring a semblance of order. The historical record presents a mixed picture of the benevolence of these groups. Several of these groups eventually deteriorated into little more than criminal gangs, or violent mobs, themselves. Others were fairly successful in bringing about a modicum of stability. One of the most notable and well documented groups was the San Francisco Committees of Vigilance. Philip J. Ethington argues that they played an essential role in shaping the path along which San Francisco’s law enforcement institutions were to develop, into what was arguably the most professional and efficient police force of the 19th century. They incorporated in their practice certain ideological elements reflective of the wider republican sentiment such as claiming to act against widespread corruption amongst public officers, or dissolving voluntarily after some months.

Helen McLure presents a different analysis of these vigilantes, highlighting the brutish and malevolent aspects of this chapter of America’s history. Nonetheless, McLure’s analysis does not preclude the plausibility that an ideologically informed order, in peculiar circumstances, is better served by deviants (who disrespect formal rules, but adhere to the ideology) than by the establishment (who respect formal rules, but are unable to implement necessary institutions, perhaps for technical or material reasons). Her focus on the role of deviant women of the Wild West, who by asserting their will and independence also shaped the future political landscape of their environment, adds credence to the relevance of deviants in shaping emerging social arrangements.
All of the Wild West was part of the jurisdictions of the various states belonging to the union. Formally there was a law-based justice system and entities charged with law enforcement. What created the demand for vigilantism was the simple fact of the vastness of the territory. The systems in place were unable to deliver justice where needed because of something similar to what ecologists call ‘scale mismatch’. The frontier was expanding at a rate that the establishment’s institutional expansion could not realistically match. The Internet is today expanding the range and space of human action at an unprecedented rate. It is very likely that the present institutional setup for delivering justice simply can not keep up. In this case, it is not a problem of reaching isolated corners of the territory that poses a problem, but the systems for categorising and conceptualising, at the institutional level, the variety of novel forms of behaviour. The average Anon is most likely an internet native. The vast amounts of resources that states expend pursuing infringers of intellectual property, deploying censorship, or even transporting leaders physically across the globe so that they may have a candid chat (something internet natives are perfectly capable of doing online), look oddly arbitrary to the Anon. From her perspective, the public prosecutors in charge of cases of rape, cyber-bullying, or financial crimes are as distant as the judges in the big cities were to the frontiersmen. The meager efforts at Open Government, or the means deployed to counter oppressive regimes, are as ineffective as the courts and the jails on the frontier. No matter how crude deviant methods for justice might seem, their superior effectiveness easily trumps the nominal availability of formal alternatives.

A similar pattern reoccurred during the Civil Rights movement, although in this case the deviance was in the form of civil disobedience rather than vigilantism.

Prior to the 1960s, the Civil Rights Movement was largely focused on achieving legal change through a sophisticated litigation program in the federal courts directed by the NAACP. Students in Greensboro, North Carolina, however, dramatically shifted the focus of the movement when they began sitting in at segregated lunch counters in February 1960—protests that were quickly replicated by student groups across the South. The initial reaction to the sit-ins among mainstream civil rights leaders and elites within the black community was largely one of disapproval.

The students at Greensboro had formal legal alternatives, but ones that compared to their deviant methods where wholly ineffective. Peñalver and Katyal’s extensive exploration of property right infringement concludes that certain instances of expressive deviance from established norms is not merely justified, but a welcome contribution to a continually evolving system of property law.

In this sense, the moral dismissal of vigilantism depends on the availability of legal or non-punitive methods of delivering justice, which are at least comparably effective as the punitive or illegal ones. From the world view of an Internet native exposed to contemporary political discourse, it is very hard to imagine how this might be so for most cases that Anonymous is involved with.
Anonymous’ normative core

Addressing the second aspect of the moral justification of Anonymous’ vigilantism—to what extent their normative position is reasonable within wider society’s moral framework—requires the assumption that Anonymous is an entity with a coherent normative core. The anthropological research offers some support for this assumption. Still, describing the ideology of Anonymous to the full extent required to answer with confidence requires much refinement of established theory and concepts. The above exploration into why Anonymous can be labelled vigilante reveals the need for an approach that:

1. does not privilege the ‘Westphalian’ state as a pre-given entity immune from critique of its very nature. (Dryzek’s Discursive Democracy approach to spaces beyond states is inspirational here; Pettit’s work provides a contrasting, state-centric, insight into underlying notions);
2. does not privilege hierarchy as a model of collaborative organisation. (Ostrom’s Institutional Analysis and Development Framework is perhaps one of the best examples of how to approach this problem);
3. adopts/uses unorthodox ethical theories to allow the translation and interpretation of online discourse. (Floridi’s IE is promising because of its affinity to ICT. More generally, a multi-theoretic approach is required.);
4. examines technologies critically through disclosive techniques. (Introna and Brey represent two alternative styles in which these techniques can be used.);
5. uses a notion of justice, including punishment, that captures expressive effects and opens up a space for deviance. (Butler’s theory of Hip-Hop punishment provides an interesting model, especially if viewed in light of justifications for civil disobedience. Feinberg also provide useful insights into the expressive function of punishment, as does Sunstein for law).

A more complete analysis of Anonymous would most certainly reveal the need for even more refinements. Until such improved analytic tools are available, the most I can claim is that Anonymous as a collective phenomenon in its present state is, at core, ideologically close to the republican ideal. This rough idea, that Anonymous, as vigilantes, fit more closely the model of the San Francisco Committees of Vigilance than that of the Ku Klux Klan, is best expressed by way of a provocative anecdote.

Those who hold the US’ Constitution’s 2nd amendment dear ought to find the Anons highly respectable characters. The analogy of cyberspace to the Wild West is even more interesting when it is looked at through the perspective of the Founding Fathers’ admiration of the frontier men. In the context of debates surrounding the 2nd amendment of the US Constitution, Shalhope shows that the right to bear arms is not only intended as a guarantee for citizens against a potential tyrannical state. It also pays tribute to the self-reliant citizen who is not averse to the idea of deploying violence to defend life, property, and community.

For the Founding Fathers, the yeoman who goes out to the frontier relying on himself and his rifle to defend his newly acquired wealth and freedom was the...
palladium of the active citizen upon which the new republic would be built. This is not to say that violence was exalted. It was the willingness to labour at maintaining order and justice that was admired, even if it meant soiling one's hands with guns. The willingness to risk one's life to protect laboriously acquired freedoms and possibilities was considered an integral part of the democratic spirit. Shalhope points out that this spirit was tied with an apparently never-ending supply of land on the frontier.

Jefferson observes that ‘our governments will remain virtuous for many centuries; as long as they are chiefly agricultural; and this will be as long as there shall be vacant lands in any part of America’. Coupled with this, however, was Jefferson’s libertarian inheritance: ‘What country can preserve it’s liberties if their rulers are not warned from time to time that their people preserve the spirit of resistance. Let them take arms’. 86

More recently, some have claimed that reality has changed the value of the firearm. Quoting Sen. Edward Kennedy, ‘our complex society requires a rethinking of the proper role of firearms in modern America. Our forefathers used firearms as an integral part of their struggle for survival. But today firearms are not appropriate for daily life in the United States’. 87 Perhaps firearms are no longer an integral part of survival because after the Information Revolution, access and use of information is what guarantees survival. In this sense, the republican spirit is very much alive and well with Anonymous. Anons are willing to violate the peace, even risk prosecution, in defence of their newly conquered territory, for their ideals of freedom. The DIY culture emerging around hackerspaces, the rising value of user-generated content, the mystique surrounding the ‘Assanges’ of this new territory, speak of the spirit of self-reliance that inspired the Founding Fathers to envision the second amendment.

Each of Anonymous’ actions has to be morally justified separately. However, the general trend is towards Ops seeking justice in conformity with a core ideology that most people living in liberal democracy would find reasonable, if not fully subscribe to. Moreover, many of these actions seek to fill a norm enforcement void arising from a scale mismatch between established institutional forms and the experience of living in an Information Society.

CONCLUSION

I have addressed the specific question are Anonymous vigilantes, and if so are they good or bad ones? My aim has not been to provide a full moral evaluation of Anonymous, but to show how engaging with online deviants may be a productive way of identifying the weaknesses in concepts underpinning moral evaluation of Internet-enabled phenomena.

The lore of the Information Revolution is replete with rags-to-riches stories where the key innovator was/is a deviant. Unfortunately, there is a general tendency to presume deviance to be negative. Merton seems to have inadvertently implied so much in his formulation of a typology of deviance. 88 Often ‘positive deviance’ is
presented as exceptional, or essentially different from other forms of deviance. Going straight from the bare fact that participating in Anonymous is deviant behaviour to the conclusion that such persons are immoral, or that the effects of Anonymous on society are necessarily negative is not only ‘empirical misrepresentation’ but also discards the potential for positive innovation that often accompanies technologically enabled deviance.89

Nowadays we use the term Luddite to mean technophobe, but the historical Luddites where not technophobes.90 Most of those involved in breaking and burning machines were operators and engineers of those same machines. Their ‘cause’ was opposition to working and trading conditions that today are clearly unacceptable (e.g. very long working hours, low quality machine-produced goods sold as genuine hand-made articles, etc.). In terms of the expanded Mertonian typology presented by Heckert & Heckert91 the Luddites were rebels as they rejected the social goals as much as, if not more than, they rejected the means to achieving them. The means they fought against—complex, large-scale machines—are still with us today, so they still would be deviants. However, the social goals they fought to establish have been fully absorbed by developed nations. Workers’ rights and health, protection against low quality counterfeits of elaborate products, etc. are now the norm.

The prankster style of Anonymous’ declarations, anonymity, distributed organisation, and other characteristics makes their iconography similar to that of the Luddites.92 While only a few Anons can be called ‘guru level hackers’, none are technophobes. To the contrary, they tend to accuse their enemies/victims of not embracing the norms implied by the technology. In this, they are the inverse of the Luddites—they are deviant innovators. Rather than rejecting the means to achieve social goals, they over-conform to them, taking the idea that digital technology permits perfect replication to its extreme normative conclusion (expressed as antagonism to Intellectual Property, demands for increased transparency from institutions and substantial protection of individuals’ privacy rights).

There is the real possibility that, just like the Luddites in the case of workers’ conditions and the value of skilled craftsmanship, Anonymous might have something significant to teach about the normative expectations of the Information Society, irrespective of the means employed. Learning from Online deviance will be very difficult without refining several morally relevant concepts. In my attempt to find out if it is OK to be an Anonymous I have applied, or hinted at, some novel conceptual approaches that can help with the needed refinements.

In the first section, I drew attention to Coleman’s investigation of this collective. This reveals that Anonymous is a complex, fluid actor. Anonymous is not as mysterious and shadowy as popular media reports would imply. In the second section, I dealt in turn with first four criteria in the definition of vigilantism. This reveals that Internet deviance raises the urgency of taking advantage of the more advanced theories of democratic statehood and collaborative action. The disclosive analysis of the digital tools used by Anonymous exposes a latent normative stance towards communal action. I also point out how IE can help us extract a meaningful moral orientation from the slogans and memes of a distributed online activity.
Anons are more like eco-warriors than like terrorists. While their actions are contentious, can seem egoistic, and can be harmful, their force is framed in a vision of common good that is not unreasonable.

Since violence is a necessary component of vigilantism, and online attacks do not physically injure or damage the target, Anonymous cannot be vigilantes according to the definition used. This is counter-intuitive and in conflict with the current use of the term. Therefore, in the third section I revisit this part of the definition. I find the inclusion of violence more problematic than helpful. A requirement of punishment is a better-suited criterion. To fulfil its function, it must be a notion of punishment that accounts for its expressive payload and the force of reprobation.

Having established that under the refined definition Anonymous are indeed vigilantes, I explore when such forms of vigilantism might be morally justified. Vigilantism is morally justified when two conditions are met: 1) no non-punitive or legal alternative is available that is comparably as effective at norm enforcement as vigilantism; and 2) the vigilante’s own moral framework, by which they justify their actions, is reasonable, i.e. it does not conflict with the moral framework of a society sharing their action space. In the last section, I draw parallels to history to argue that in very general terms the first condition is likely to be met in several of Anonymous’ Ops. Examining the second condition can only be done reliably once the conceptual refinements demanded by the information age are at hand. There are, however, significant incitations that the ideological frameworks of Anonymous and the citizens of liberal democracies are on converging paths of evolution.

This is not to say that specific actions cannot be considered immoral, or that particular individuals are not guilty of immoral reprehensible acts under the banner of Anonymous. When specific acts can be clearly identified as unacceptable the perpetrators must be brought to justice. Anonymous, as all vigilantes, seeks to punish infringers, and so harm individuals, even if not through violence. Too many times in the past have vigilantes adopted a skewed sense of justice and harmed the innocent. While my appraisal of Anonymous is generally positive, that only applies to those actions motivated by the right sense of justice.

Ultimately, being an Anonymous is OK. One does not have to participate in every Op, adopt the full gamut of practices, nor approve of all activities to be an Anon. Such is the permeable nature of this fluid entity. When the just enforcement of norms is drastically under-served, vigilantism may be a reasonable undertaking. This will often involve breaking the law, and as with civil disobedience, Anons must be ready (if unwilling) to face the unpleasant consequences of their struggle for justice. Anonymity does not equate to immunity, as some naïve netizens sometimes believe.

Anonymous is but the strong-arm of an ethos that is becoming ever more relevant to netizens, and any others affected by the Internet. The ideological grounding to this ethos is neither new, nor radically alternative. But it is wrapped in, and expressed through, technological mediation making it hard to interpret. Considering that exploration of deviant behaviour such as Anonymous can accentuate the conceptual frameworks undergirding Information Society, even if one ultimately disapproves of its activity, demonising the phenomenon is unwise.
Is it OK to be an Anonymous?

NOTES


5. Anon is the singular of Anonymous. This meaning is in contrast to the more straightforward concept of member. Since the idea of membership is problematic for this collective, I use its own terminology.

6. I propose the Portuguese Man O’ War to be an even more apt metaphor. This creature looks and behaves very much like a jellyfish, but it is not one. It is what biologists call a composite organism. Each part of the creature is a distinct organism, each with its own specialisation. The creature exists as a tight symbiotic relationship of its constituent but distinct parts. Unlike the Hydra, this creature is not intrinsically evil, but is nevertheless very dangerous and must be handled carefully. It is also very real, not mythological. While it is perfectly reasonable to speak of Anonymous, or of a Portuguese Man O’ War, as a unitary entity, focusing on certain aspects of the phenomenon/entity also makes sense, and, for the purposes of analysis, may be more fruitful.


8. Ibid.


10. Free as in without restrictions to access or use, not simply without cost. This struggle for information liberation can stretch from whistle blowing and leaks all the way to content piracy.

11. This already reveals an aspect of Anonymous that distinguishes them from other subversive groups, and shows affinity to a rudimentary democratic spirit.


15. A single action is called an ‘Op’ by Anonymous; a contraction of the military term ‘Operation’.


20. Ibid., 58.


26. By netizens I mean persons who use Internet technology to an extent that it is an integral and valuable part of their daily life. These individuals would need to make major changes to their lives, and go through a painful adjustment period, if deprived of Internet accessibility. They are not necessarily computer nerds, or highly skilled in programming. Most are not. A ‘life online’ might consist of long hours of gaming, gossiping on social networks, using the Internet on a smart phone to interact with others, or full dependence on the Internet for work. I do not consider a netizen one who only uses the Internet occasionally, or for phone calls via Voice over IP.


37. Floridi’s use of the term entropy is not the same as in physics. Information entropy indicates the inverse of flourishing of information objects. Information entropy is to an information object what ‘nothingness’ is to ‘being’. In this sense censorship, excessive secrecy, misrepresentation and misinformation can all be conceived of as entropy promoting activities.


41. The ‘lowc—LOIC web version with HiveMind’ [sic] is available from http://code.google.com/p/lowc/. It consists of an HTML page with some JavaScript. It is more rudimentary than the original, but since it does not require the user to download software it is easier to deploy massively. Developing such tools indicates the willingness of some Anons to open up and widen the community to those who are less tech-savvy. See also Steve Mansfield-Devine, ‘Anonymous: Serious Threat or Mere Annoyance?’ Network Security 2011, no. 1 (January 2011): 4–10, doi: 10.1016/S1353-4858(11)70004-6.


43. The Low Orbit Ion Cannon source code is available at https://github.com/NewEraCracker/LOIC/ (README file as of commit e514e9d). A botnet is a network of programs running on different computers which can be remotely controlled and coordinated by the user who deploys the botnet. Botnets typically (but not necessarily) run on computers compromised through a virus, without the owner of the computer being aware, or approving, of his/her system being used for such purposes.


45. Forgoing the multimedia capabilities of today’s computers, using only terminal type, renders a nostalgic retro styling in most digital contexts.

50. According to Johnston the credible threat of violence is sufficient to qualify an action as vigilante. Even if Anons have used threats of physical harm, most of these are not sufficiently credible, nor are they a core characteristic of the phenomenon. I use the term violence to mean ‘violence and/or a credible threat of violence’.
51. One could argue that the Stuxnet computer worm that interferes with centrifuges’ controls to cause physical damage, and might have caused problems to Iran’s nuclear research program, is a digital expression that causes real physical damage. This is a rather different class of digital attack than the ones undertaken by Anonymous, and does not involve voluntary public participation or publicity. The issue of effects across the cyberspace/real-world divide is addressed in Johnny Hartz Søraker, ‘Virtual Worlds and Their Challenge to Philosophy: Understanding the “Intravirtual” and the “Extravirtual”’, Metaphilosophy 43, no. 4 (2012): 499–512, doi: 10.1111/j.1467-9973.2012.01755.x.
54. Ibid., 296.
57. Ibid., 398.
65. The website http://www.legal-walls.net/ provides a service for finding and listing such legal graffiti walls.


68. The idea that there are strong parallels between the Wild West and cyberspace is neither new nor immune from criticism. See McLure, ‘The Wild, Wild Web’ for a detailed analysis of the analogy as it was used before the days of Anonymous.


75. In view of the case of Anonymous (and perhaps Wikileaks) that conclusion could be extended to laws covering expressions in general.


78. Ostrom, *Understanding Institutional Diversity*.


80. Introna, ‘Maintaining the Reversibility of Foldings’.


82. Butler, ‘Much Respect’.

83. As Anonymous, like almost all online phenomena, is a rapidly evolving one, any claim is susceptible to become invalid as the phenomenon morphs into something else, while retaining the original label.


85. This alone would already provide for some argument for the right to deploy DDoS as the cyber-gun of a cyber-militia defending its integrity.


87. Ibid.


P. Serracino-Inglof


91. Heckert and Heckert, ‘Using an Integrated Typology of Deviance to Expand Merton’s Anomie Theory’, 81, 86.

92. For example, the leader of the Luddites was a fictitious character ‘King Ludd’ inspired by a story of an oppressed individual who vents his anger by smashing the machine. Anonymous have adopted the mask of the character V from the film Vendetta, which is in turn inspired by Guy Fawkes; Rosie Waites, ‘The Man Behind the V for Vendetta Mask’, *BBC*, October 20, 2011, http://www.bbc.co.uk/news/magazine-15359735. In both cases, the true story of an individual turning violent to strive for freedom (in vain) becomes a fictive character, then the face of a movement. Also, the Luddites (or rather their cause) even had sympathisers in the British Parliament. The Pirate Party, which is becoming rather successful throughout Europe, shares concerns with Anonymous (without necessarily supporting their methods) on Intellectual Property and privacy; Juli Zeh, ‘The Pirate Party Fits the Political Gap’, *The Guardian*, May 18, 2012, http://www.guardian.co.uk/commentisfree/2012/may/18/germany-pirate-party-political-gap.